

*Latvijas Nacionālās informācijas tehnoloģiju drošības incidentu  
novēršanas institūcijas CERT.LV veidošana*

Baiba Kaškina, Katrīna Sataki - CERT.LV/CERT NIC.LV  
Rīga, 2011.gada 8.februāris  
LU 69.konference



CERT **NIC**.LV

# *Saturs*

- Ievads
- Situācijā Latvijā agrāk
- Jaunais IT drošības likums
- CERT.LV veidošana

*levads*

## *Termini*

**CERT –**

**Computer Emergency Response Team**

**CSIRT -**

**Computer Security Incident Response Team**

## *Par ko CSIRTi uztraucas?*

- Uzbrukumi infrastruktūrai
- DoS, DDoS
- Botneti
- Phishing
- Pharming
- Autortiesību pārkāpumi
- Sociālā inženierija
- Urķēšanās – hacking
- Nokalušīšanās – sniffing
- Mēstules – SPAM
- Trojāni, vīrusi, tārpi
- Uzlauzti (kompromitēti) datori, konti
- ...

## *Kā CSIRTi darbojas?*

- RFC-2350: “*Expectations for Computer Security Incident Response*”
- Atsevišķa organizācija, nodaļa vai pāris cilvēki nepilnā slodzē
- CSIRT ir klientūra – IP adresu apgabals vai AS, ko viņi pārvalda

# *Situācija Latvijā āgrāk*

## ***CERT NIC.LV***

- LU MII Tīkla risinājumu daļas sastāvā
- Dibināts 2006.gadā ar nosaukumu LATNET CERT
- Trusted Introducer akreditācija – 2008
- FIRST akreditācija – 2009
- Sadabība – TF-CSIRT, ENISA, citu valstu CSIRT komandas



## ***CERT NIC.LV Klientūra***

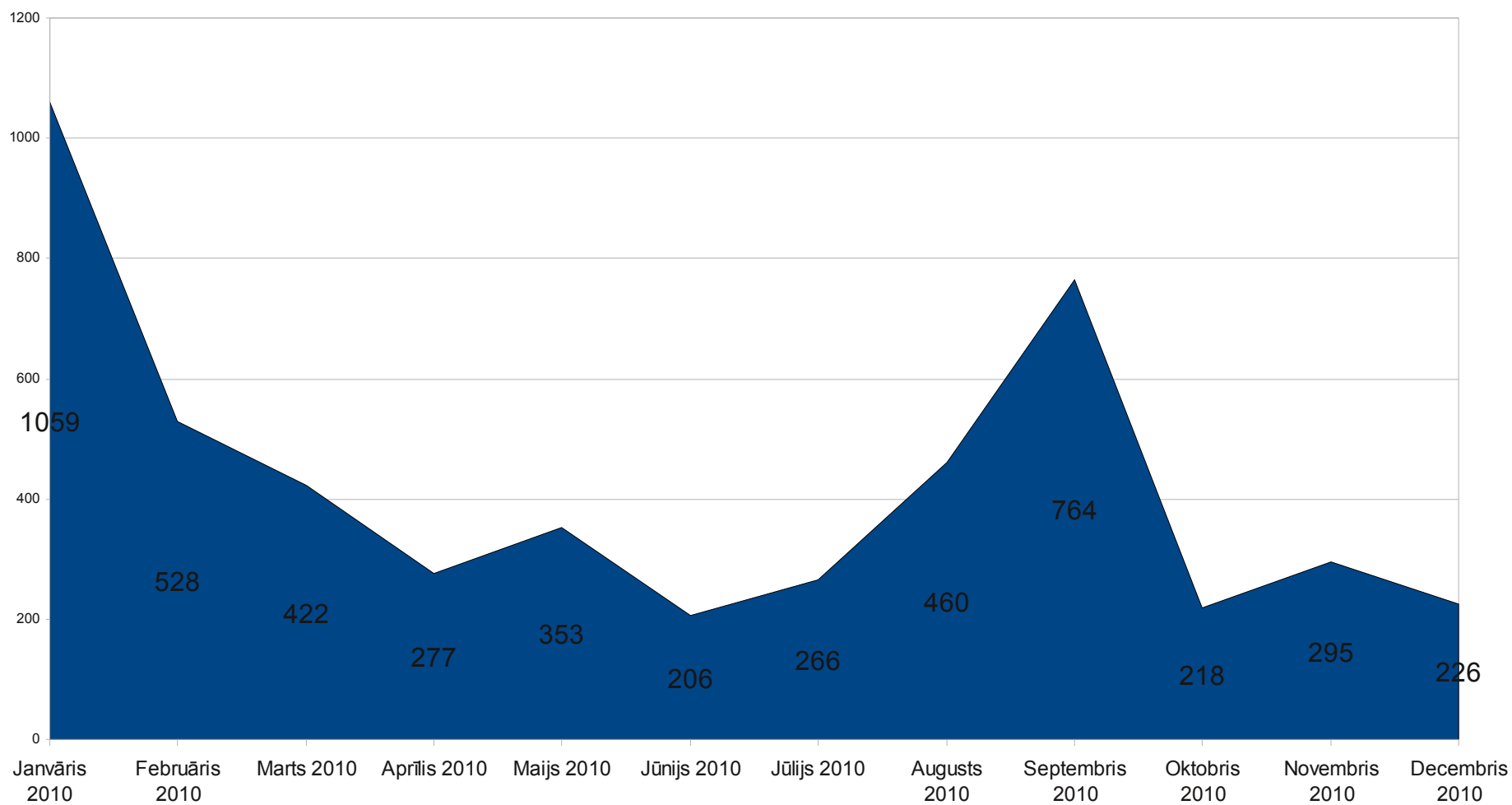
- Akadēmiskais tīkls
  - GÉANT pieslēgums 2,5 Gb/s
- LU MII datu centrs, klienti
- DNS drošības jautājumi
- Organizācijas, ar kurām noslēgts sadarbības līgums
- Incidentu koordinēšana starp dažādām institūcijām valstī

## ***DDIRV***

- Izveidota 2007
- TI akreditācija 2008
- Klientūra – valsts un pašvaldību institūcijas

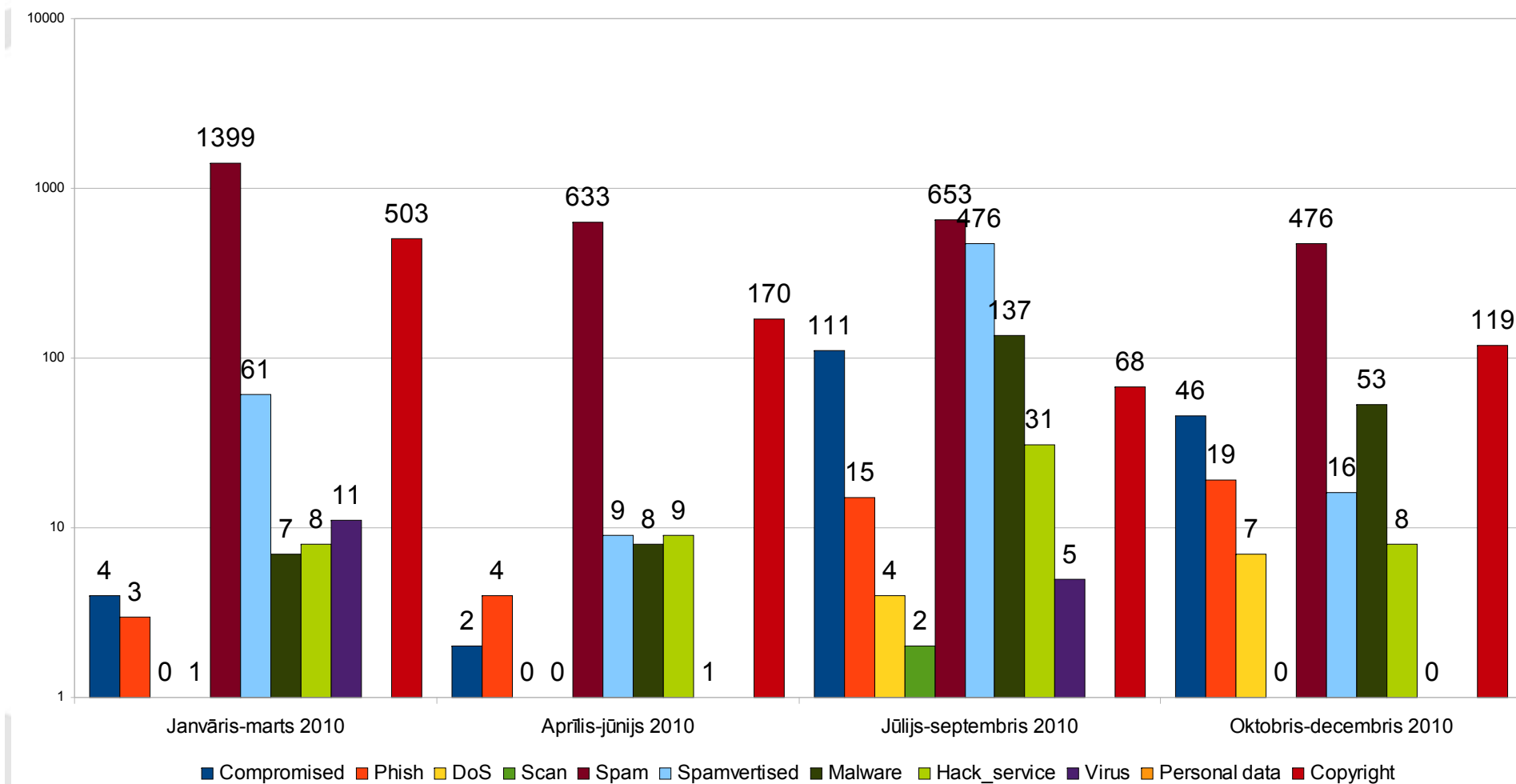
# CERT NIC.LV incidenti 2010.gadā

Incidentu skaits

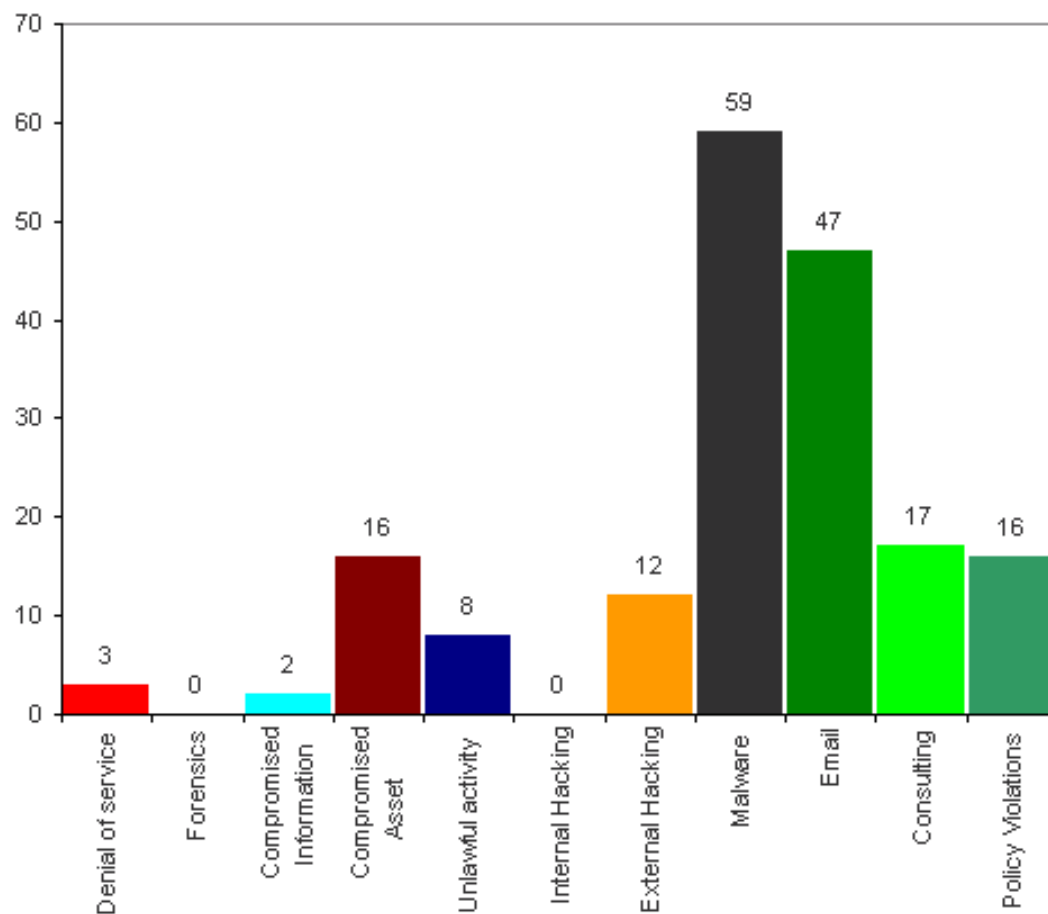


# CERT NIC.LV incidentu tipi 2010.gadā

Incidentu tipi un skaits



## *DDIRV incidenti 2010.gadā*



# ***Jaunais IT drošības likums***

## *IT drošības likums*

- Pieņemts 2010.gada 28.oktobrī
- Stājas spēkā 2011.gada 1.februārī
- Izveido Latvijas Nacionālo Informācijas tehnoloģiju drošības incidentu reaģēšanas institūciju LU MII

## *Likuma mērķis*

Uzlābot informācijas  
tehnoloģiju drošību  
Latvijā



## *Izveido*

Latvijas Nacionālo Informācijas  
tehnoloģiju drošības incidentu  
reaģēšanas institūciju –  
CERT.LV

## *Uzliek pienākumus un tiesības*

- CERT.LV
- Valsts un pašvaldību institūcijām
- Privātajam sektoram

## *CERT.LV pienākumi*

- Uzturēt vienotu elektroniskās informācijas telpā notiekošo darbību atainojumu
- IT drošības incidentu risināšana
- Rekomendācijas sabiedrības izglītošana
- Pētniecība drošības jomā
- Sadarbība ar citām CSIRT vienībām

## ***CERT.LV tiesības***

- Pieprasīt un saņemt informāciju par incidentiem
- Monitorēt
- Veikt kritiskās infrastruktūras pārbaudes
- Pieņemt lēmumus (izdot administratīvus aktus) – lai nodrošinātu likuma izpildi
- Pieprasīt atslēgt gala lietotājam internetu līdz 24h

***CERT.LV***

***CERT.LV***

**CERT NIC.LV + DDIRV**

## **CERT.LV**

- Valsts finansējums
- Satiksmes ministrija pārrauga
- Jāpilda IT drošības likums (piešķirtā budžeta ietvaros)
- 10 cilvēki, ~4,5 PLE
- Pieredze no abām CSIRT komandām
- Sadarbība – TF-CSIRT, FIRST, TI, ENISA, NATO, ...

## *CERT.LV plāni*

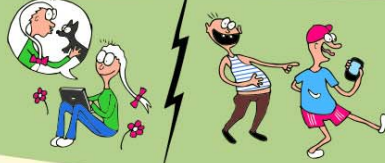
- Izglītojoši plakāti un portāls
- Cieša sadarbība ar valsts un pašvaldību iestādēm
- Mācības, vingrinājumi
- Semināri



# Vai esi Interneta profiņš?

## Apdomā pirms publisko attēlus internetā!

Padomā, vai šie attēli neaizskar un nekaitē Tev, Taviem draugiem, klasesbiedriem, vecākiem vai jebkuram citam cilvēkam, kas attēlots fotogrāfijā. Pēc tam, kad attēls ir „ielikts“ internetā, to vairs nevar iznīcināt vai padarīt par nebijušo.



## Lieto drošas paroles!

Katram portālam izmanto savādāku paroli. Veido to pietiekami sarežģītu, lai to nevarētu uzminēt pat tie cilvēki, kas Tevi labi pazīst!



## Neatklāj datus par sevi nepazīstamiem cilvēkiem!

Nebūt ne visi, ko Tu satiec virtuālajā vidē, ir tie, par ko uzdodas. Bieži vien (jaundarī slēpj) savu patieso seju, lai vieglāk piekļūtu Tev, Taviem radīem un draugiem. Jo vairāk Tu par sevi atklāsi, jo vieglāk viņi varēs nodarīt Tev pāri reālajā dzīvē. Neatklāj, kā Tevi sauc, kur Tu dzīvo, kas ir Tavi vecāki vai kādas mantas Tev ir mājās.



## Nesarunā tikšanās ar tīklā satiktajiem pazīpām!

Atceries, ka tīklā satiktie cilvēki ne vienmēr ir tie, par ko izliekas! Sargā sevi, lai neviens nevar nodarīt Tev pāri! Nepiekrīti tikties ar nepazīstamiem cilvēkiem nomaļās vietās, kur nav neviena, kas nepieciešamības gadījumā varētu Tev palīdzēt.



## Darbības internetā nav anonīmas!

Tavas darbības internetā nav anonīmas! Vajadzības gadījumā tām var izsekot gan skolotāji, gan vecāki, gan likumu sargājošas iestādes.



## Neraksti aizskarošus komentārus!

Cilvēki, kas aizvaino citus, paši jūtas nelaimīgi. Taču, aizvainojot citus, neviens laimīgāks nekļūst. Nesāpini apkārtnes! Est iecietīgs pret citu viedokli, dzīvesveidu, dzīves uzskatiem.



## Mēstules nav vēstules!

Ignorē mēstules, ko saņem nepazīstamiem cilvēkiem. Neatsaucies to „vilinošajiem” piedāvājumiem. Visbiežāk tie ir mēģinājumi izkrāpt Tavu naudu. Mēstules var izfiltrēt un par tām var sūdzēties.



## Neiepērcies internetā bez vecāku ziņas!

Nesniedz internetā savas vai vecāku kredītkartes datus, iepriekš neapspriežoties ar vecākiem. Atceries - izmantojot kredītkartes datus, var nozagt visu naudu, kas pieejama ar šo karti.



## Rūpējies par datora veselību!

Neinstalē nezināmas izcelsmes programmas uz datora, ko Tu lieto. Programma ļoti viegli var izlikties par spēli, bet patiesībā būt vīruss, kam Tu pats paver ceļu uz savu datoru.



## Ja Tu:

- saņem nepatīkamas, aizvainojošas vēstules internetā,
  - esi saskāries ar nepatīkamiem materiāliem internetā,
  - esi pamanījis aizdomīgas darbības internetā,
  - esi satraukts par savu drošību internetā,
- pastāsti par to saviem vecākiem vai kādam citam no pieaugušajiem, kam uzticies! Vari zvanīt Bērnu un jauniešu bezmaksas uzticības tālrunim 116111 vai rakstīt uz: zinojumi@drossinternets.lv vai abuse@nic.lv

**Jūsu darbības internetā nav anonimas!**

Tām var izsekot gan likumu sargājošas iestādes, gan Jūsu interneta pakalpojumu sniedzējs vai darba devējs.

OK

**Nerakstiet e-pastā, diskusiju forumā vai komentāros to, ko Jūs nerakstītu uz papīra!**

Aizvainojot citus, labāki nekļūstat.

Labi

**E-pasta vēstule, kas nosūtīta no Jūsu datora, nepazūd nebūtībā.**

Tās kopijas saglabājas daudzās vietās un tās var izlasīt arī cilvēki, kuriem vēstule nav tikusi adresēta.

OK

**Domājiet par sava datora drošību!**

Izmantojiet pretvīrusu programmatūru, lai pasargātu savu datoru un tajā saglabāto informāciju no bojāšanas, zuduma vai nokļūšanas nepiederošu personu rokās.

OK

**Pārdomājiet, kādas fotogrāfijas publicējat internetā un kā to publicēšana kādu dienu var ietekmēt Jūsu dzīvi!**

Piemēram, attiecības ar draugiem, radniekiem, kolēģiem, esošajiem vai nākamajiem darba devējiem.

OK

**Ne Jūsu banka, ne kāds cits pakalpojumu sniedzējs nekad neizmantos e-pastu, lai noskaidrotu Jūsu paroles, pin kodus vai kodu kartes datus.**

Ja saņemat e-pasta vēstuli, kurā bankas vai kāda cita vārdā Jums tiek prasīts norādīt savas paroles, nekavējoties informējiet par to banku vai citu organizāciju un nekādā gadījumā nesniedziet nevienam savu slepeno informāciju.

Labi

**Īpaši svarīgas vai sensitīvas informācijas datu pārsūtīšanai izmantojiet kriptēšanu – PGP.**

Visa informācija par to atrodama internetā.

OK

**Uzmaniet bērnus, kas darbojas internetā, sociālajos tīklos, sarakstās ar tīklā iepazītiem cilvēkiem.**

Neesiet vienaldzīgi! Pārlicinieties, ka bērni ir informēti par to, kā jāuzvedas internetā, ko drīkst un ko nevajadzētu darīt.

Labi

**Pirkumiem internetā labāk izmantojiet atsevišķu kredītkarti, uz kuras uzskaitiet tieši tik naudas, cik nepieciešams konkrētā pirkuma veikšanai.**

Tas pasargās Jūs no krāpniekiem, kas vēlēšies izmantot Jūsu kredītkarti saviem pirkumiem.

OK

**Pirms veikt pirkumus internetā pārlicinieties, vai attiecīgās mājas lapas īpašniekam var uzticēties!**

Palasiet, ko par tirgotāju saka citi interneta lietotāji. Pirms levdāt savas kredītkartes datus pārlicinieties, ka mājas lapā tiek izmantots drošs savienojums, t.i. pirms mājas lapas adreses ir burti <https://> un pārlūkprogrammas apakšējā stūrī redzama ikona, kas norāda uz drošu savienojumu.

Labi

**Izslēdziet pa nakti savu datoru!**

Tā ietaupīsiet gan elektrību, gan samazināsiet risku, ka Jūsu dators tiek uzlauzts.

OK

**Aizsargājiet sev svarīgos datus ar paroli!**

Paroli izvēlieties pietiekami sarežģītu, lai to nevarētu uzminēt pat cilvēki, kas Jūs labi pazīst. Dažādos portālos lietojiet dažādas paroles! Izstrādājiet savu sistēmu, kā tās atcerēties vai arī izmantojiet kādu no drošajām paroli glabāšanas programmām!

OK

*Paldies!*

**baiba@cert.lv**

**cert@cert.lv**

**www.cert.lv**